AZ-104Q&As

Microsoft Azure Administrator

Pass Microsoft AZ-104 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/az-104.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

You sign up for Azure Active Directory (Azure AD) Premium.

You need to add a user named admin1@contoso.com as an administrator on all the computers that will be joined to the Azure AD domain.

What should you configure in Azure AD?

A. Device settings from the Devices blade.

B. General settings from the Groups blade.

C. User settings from the Users blade.

D. Providers from the MFA Server blade.

Correct Answer: A

When you connect a Windows device with Azure AD using an Azure AD join, Azure AD adds the following security principles to the local administrators group on the device:

1.

The Azure AD global administrator role

2.

The Azure AD device administrator role

3.

The user performing the Azure AD join

In the Azure portal, you can manage the device administrator role on the Devices page. To open the Devices page:

1.

Sign in to your Azure portal as a global administrator or device administrator.

2.

On the left navbar, click Azure Active Directory.

3.

In the Manage section, click Devices.

4.

On the Devices page, click Device settings.

5.

To modify the device administrator role, configure Additional local administrators on Azure AD joined devices.

References: https://docs.microsoft.com/en-us/azure/active-directory/devices/assign-local-admin

QUESTION 2

HOTSPOT

You have an Azure subscription.

You plan to use an Azure Resource Manager template to deploy a virtual network named VNET1 that will use Azure Bastion.

How should you complete the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
{
"type": "Microsoft.Network/virtualNetworks",
"name": "VNET1"
"apiVersion": "2019-02-01",
"location": "[resourceGroup().location]",
"properties": {
"addressSpace": {
"addressPrefixes": ["10.10.10.0/24"]
},
"subnets": [
{
        "name": [AzureBastionSubnet | AzureFirewallSubnet | LAN01 | RemoteAccessSubnet]
        "properties": {
          "addressPrefix": [10.10.10.0/27 | 10.10.10.0/29 | 10.10.10.0/30]
        }
      },
      {
          "name": "LAN02",
          "properties": {
              "addressPrefix": "10.10.10.128/25"
          }
      }
    ]
  }
}
```

Correct Answer:

Answer Area

```
{
"type": "Microsoft.Network/virtualNetworks",
"name": "VNET1"
"apiVersion": "2019-02-01",
"location": "[resourceGroup().location]",
"properties": {
"addressSpace": {
"addressPrefixes": ["10.10.10.0/24"]
},
"subnets": [
{
        "name": [AzureBastionSubnet | AzureFirewallSubnet | LAN01 | RemoteAccessSubnet]
        "properties": {
          "addressPrefix": [10.10.10.0/27 | 10.10.10.0/29 | 10.10.10.0/30]
        }
      },
      {
          "name": "LAN02",
          "properties": {
              "addressPrefix": "10.10.10.128/25"
          }
      }
    ]
  }
}
```

Reference: https://medium.com/charot/deploy-azure-bastion-preview-using-an-arm-template-15e3010767d6

QUESTION 3

You are the global administrator for an Azure Active Directory (Azure AD) tenet named adatum.com. You need to enable two-step verification for Azure users. What should you do?

A. Create a sign-in risk policy in Azure AD Identity Protection

B. Enable Azure AD Privileged Identity Management.

C. Create and configure the Identity Hub.

D. Configure a security policy in Azure Security Center.

Correct Answer: A

Identity Protection analyzes signals from each sign-in, both real-time and offline, and calculates a risk score based on the probability that the sign-in wasn\\'t performed by the user. Administrators can make a decision based on this risk score signal to enforce organizational requirements. Administrators can choose to block access, allow access, or allow access but require multi-factor authentication. If risk is detected, users can perform multi-factor authentication to self-remediate and close the risky sign-in event to prevent unnecessary noise for administrators. With Azure Active Directory Identity Protection, you can:

1.

require users to register for multi-factor authentication

2.

handle risky sign-ins and compromised users

References: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/flows

QUESTION 4

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result these questions will not appear in the review screen.

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Region
RG1	Resource group	West US
RG2	Resource group	East Asia
storage1	Storage account	West US
storage2	Storage account	East Asia
VM1	Virtual machine	West US
VNET1	Virtual network	West US
VNET2	Virtual network	East Asia

VM1 connects to VNET1.

You need to connect VM1 to VNET2.

Solution: You delete VM1. You recreate VM1, and then you create a new network interface for VM1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Instead you should delete VM1. You recreate VM1, and then you add the network interface for VM1. Note: When you create an Azure virtual machine (VM), you must create a virtual network (VNet) or use an existing VNet. You can change

the subnet a VM is connected to after it\\'s created, but you cannot change the VNet.

References:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/network-overview

QUESTION 5

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription named Subscription1. Subscription1 contains a resource group named RG1. RG1 contains resources that were deployed by using templates.

You need to view the date and time when the resources were created in RG1.

Solution: From the RG1 blade, you click Automation script.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

From the RG1 blade, click Deployments. You see a history of deployment for the resource group.

Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/template-tutorial- create-first-template?tabs=azure-powershell Through activity logs, you can determine:

1.

what operations were taken on the resources in your subscription ?who started the operation

2.

when the operation occurred

3.

the status of the operation

4.

the values of other properties that might help you research the operation

1.

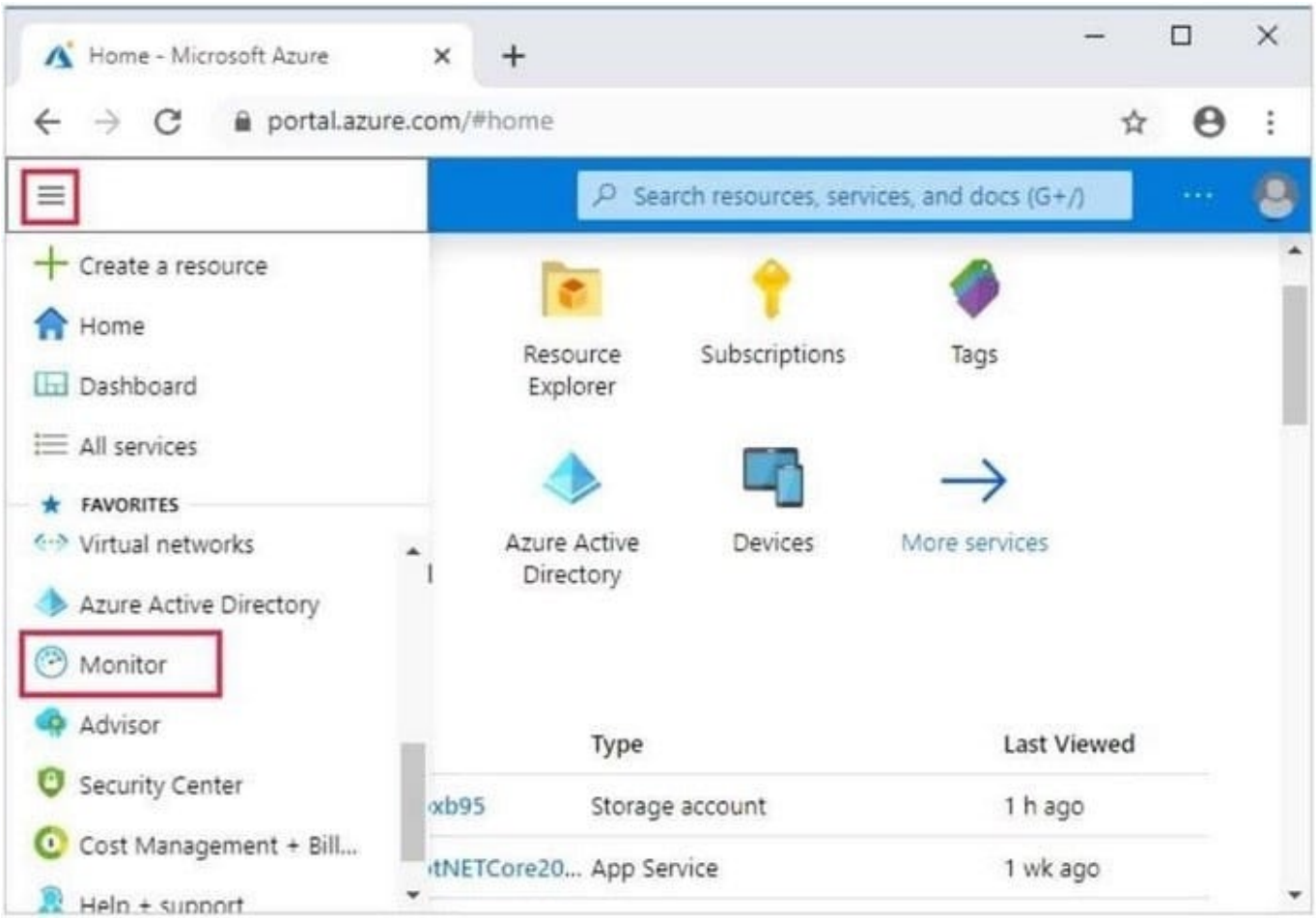
On the Azure portal menu, select Monitor, or search for and select Monitor from any page

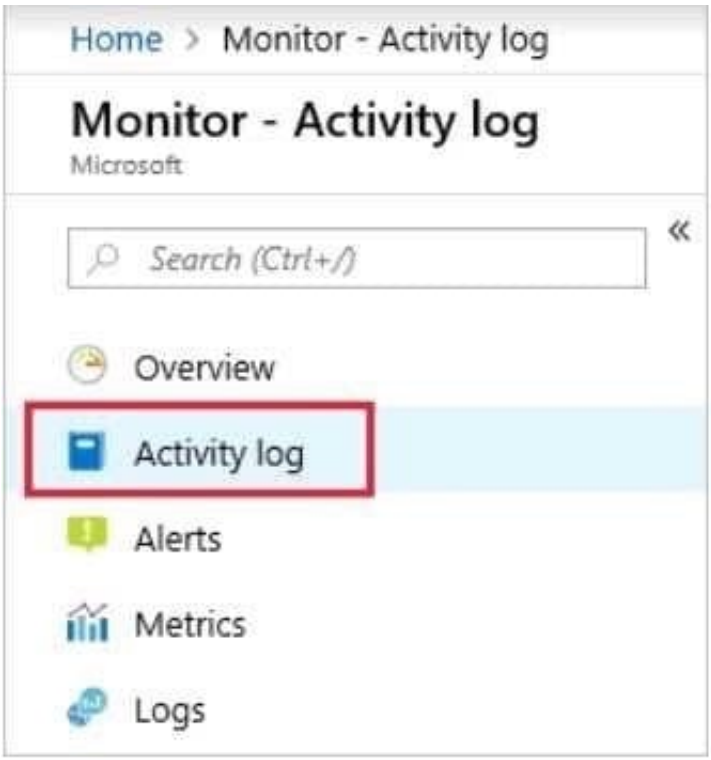
2.

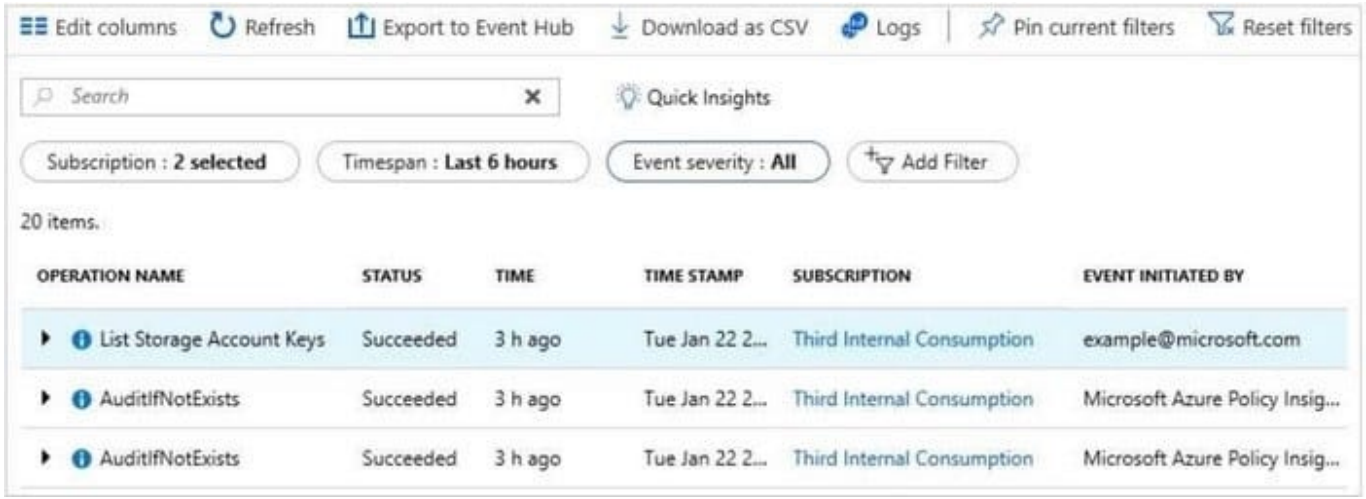
Select Activity Log.

3.

You see a summary of recent operations. A default set of filters is applied to the operations. Notice the information on the summary includes who started the action and when it happened.


Home - Microsoft Azure
portal.azure.com/#home
Search resources, services, and docs (G+/)
Create a resource
Home
Dashboard
All services
FAVORITES
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Bill...
Help + support
Resource Explorer
Subscriptions
Tags
Azure Active Directory
Devices
More services
Type
Last Viewed
xb95
Storage account
1 h ago
tNETCore20...
App Service
1 wk ago


Home > Monitor - Activity log
Monitor - Activity log
Microsoft
Search (Ctrl+/)
Overview
Activity log
Alerts
Metrics
Logs



Reference: https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/view-activity-logs